APL#10131

RECONASENSE

PHYSICAL SECURITY'S TECHNICAL TOOLKIT

FOR INSIDER THREAT DETECTION & MITIGATION (ITDM)

Today's physical security landscape is filled with increasingly sophisticated threats and ongoing attacks, so protecting people, assets, and buildings demands high functioning, proactive security. As security infrastructures expand to include more mobile, cloud, IoT, building automation, and non-security applications, the amount of available data to analyze is exploding. Security teams monitor more systems than ever before and try to detect, respond, and mitigate threats in real-time. In many cases, these systems are outdated, lack interoperability, scalability, and do not provide real-time, actionable intelligence.

To be more effective, physical security management and access control solutions must take an integrated and proactive security approach. They must enable the flow of business and productivity while actively monitoring and assessing security risks. They must ensure compliance and enforce policy while capturing all activity and keeping it available for forensic and audit reporting needs.

With the increased amount of data, the growing number of connected humans, devices, and facilities to manage, simply adding more surveillance and forensic capabilities won't effectively minimize risk, nor will it help security teams take the right action during an attack. Government facilities and installations need an intelligent, interoperable approach to threats that is risk-based and contextually aware to provide actionable intelligence from all connected data sources.

ABOUT RECONASENSE

DESIGNED TO FEDERAL SPECIFICATIONS

ReconaSense is the first COTS Risk-Adaptive security framework that helps protect federal, military, critical infrastructure and other sensitive facilities requiring top-grade security. Our patented solution meets and exceeds Government regulations for HSPD-12, FIPS 201, ICD705, UL1076, and FIPS 140-2.

Developed and designed as a suite of risk-mitigating security solutions, ReconaSense meets federal agencies' highest level of requirements. The ReconaSense framework was specifically architected to secure a wide range of sensitive applications across the military, government, and critical infrastructure spaces. Combining its dedicated team of security professionals and engineers with decades of experience securing such facilities and their open network architecture, ReconaSense identifies risks and helps mitigate potential threats and attacks before they happen. Its predictive nature and interoperability enable security teams to achieve unprecedented situational awareness and rapid response capabilities.

SIA NEW PRODUCT SHOWCASE
Access Control Software & Controllers
AWARD

Securing Critical Sectors:

Military, Federal and State Governments

Ports and Critical Infrastructure

Commercial

Industrial

Corrections

ReconaSense framework delivers a revolutionary security platform for federal and critical infrastructures. It combines unified data with intelligent risk-adaptive controls, actionable guidance, and new integrations with IoT sensor technology and building automation.

Significantly improving safety, we keep sensitive facilities secure and valued people and assets protected.

SYSTEM ARCHITECTURE: FICAM EMBEDDED

By leveraging the HID pivCLASS® solution, the ReconaSense framework integrates the HID pivCLASS® authentication module (PAM) technology directly into the Mercury Security LP4502 controller. The Public Key Infrastructure (PKI) validation certificate is embedded in the controller and occurs real-time when a credential is presented at the reader.

ReconaSense supports up to 16 FICAM readers per LP4502 by using the 2 reader ports on the LP4502 and up to 14 additional PIV readers via downstream devices using the MSC sub-controllers.

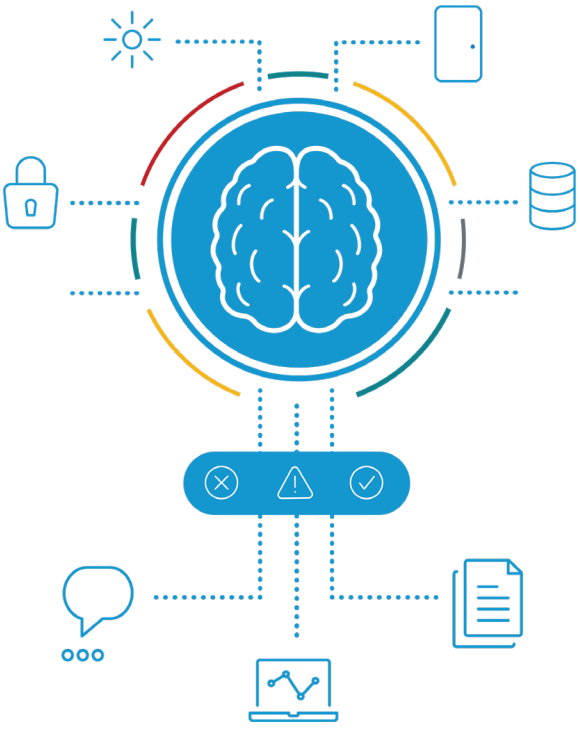
UNIFIED ACROSS THE ENTERPRISE

BREAK DOWN DATA SILOS ACROSS FEDERAL SYSTEMS WITH TRUE UNIFICATION

At the core of ReconaSense's software solution is the unification platform. For PACS that need to extend across several sites under one central agency, our system unifies and syncs all modifications, updates, and adjustments made in one system. Credential registrations, employee and contractor enrollments made in one site will adjust automatically across the enterprise. When access privileges are modified, a termination occurs, or certifications expire, changes sync across all areas.

With an open architecture capable of integrating with virtually any sensor, system, or data source, ReconaSense translates data across security technologies into one common language, on one common operating platform, providing a clear view of risks. Most importantly, the system can act automatically to adjust permissions informed by intelligent data. Whether unifying access control, video systems, intrusion detection, IoT sensors, mobile capabilities, building automation systems, and more, ReconaSense delivers a seamlessly unified operation that provides intelligent security insights and actionable data.

The ReconaSense unified security platform integrates with all federal security systems and other applications at the database layer, translating data and delivering security intelligence through a single interface. By breaking down the barriers and silos between the multitude of systems, you can have a more intelligent view into security across your entire operation.



UNIFY DISPARATE SOURCES OF DATA

SCALEABLE & SIMPLE TO USE

BUILT FOR SECURITY OPERATIONS OF ANY SIZE AND COMPLEXITY

Understanding the ever-evolving challenges security operators across the military and government face, the ReconaSense engineering team built a highly flexible and scalable solution meant to adapt to changes instantly and with ease. Whether managing physical security for one site or hundreds, the system adapts and adjusts in real-time to any security risk, trigger, certification update, and/or custom security protocol.

INTUITIVE, USER-DEFINED CAPABILITIES

The ReconaSense unification framework is a fully customizable, commercial-off-the-shelf (COTS) solution. This capability provides a truly one-of-the-kind and robust PACS experience for the user, raising the bar for flexibility and ease-of-use to meet most any access control or physical security requirement.

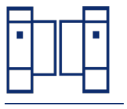
TURNING INTELLIGENT DATA INTO ACTION

ADVANCED ACCESS CONTROL WITH AN INTELLIGENT, RISK-ADAPTIVE APPROACH

ReconaSense takes a significant step forward in security technology by doing more than reporting on security events after they occur. For the first time, security operators can do more than scrutinize security data after an incident occurs. The ReconaSense framework provides a mechanism to count and score data inputs and security activity. This scoring process is a sophisticated mechanism that enables identifying growing risks and threats at a facility in real time.

Risk is different than traditional policy breaches within a secure environment. Risk is the emerging threat as the activity occurs and increases or decreases based on types of activity. Risk is not readily identifiable and not easily calculated across a unified platform in legacy access control and physical security systems. ReconaSense calculates risk as part of the built-in processes and protocols.

Risk-Adaptivity is identified through a multitude of proprietary ReconaSense framework capabilities. These proprietary capabilities include:



Risk-Adaptive Physical Access Control System (RAdPACS)

RAdPACS provides modern enterprise-wide management and enforcement capabilities for physical access privileges. It modernizes the management of credential enrollment, validation, verification, authorization, mitigation, and revocation of physical access credentials. The real-time evaluation of situational awareness data drives corresponding risk-adaptive adjustment of access levels to ensure policy compliance.

According to real-time risk-based analysis, this effort allows facilities to improve safety, security, and efficiency with automatic adjustments of physical access privileges.

Risk-Adaptive Command Control Display (RAdCCD)

RAdCCd provides enterprise-wide management and enforcement capabilities for physical security operations. It modernizes the management of roles, responsibilities, and rules across security personnel, security material and security information to reflect real-time risk levels. Risk-based evaluation of situational awareness allows operators to automatically adjust security management according to real-time security risks or threats.

RAdCCD was designed to improve operational effectiveness, installation resilience, and threat detection capabilities for militarygrade facilities using COTS components.

Risk-Adaptive Insider Threat Intelligence & Interception (RAdInT)

RAdInT provides enterprise-wide monitoring and enforcement capabilities to prevent, detect, and mitigate physical Insider Threat (InT) attacks.

RAdInT modernizes installation security postures against internal unauthorized physical access, including rogue badges and operator collusion. By using risk-based analysis and risk-adaptive controls, decision-makers can more effectively prevent and report suspected physical InT activity. For the first time, security operations can verify fitness and evaluate the purpose surrounding physical access requests based on real-time situational awareness data.

UNRIVALED SECURITY TECHNOLOGY

360˚ COVERAGE OF YOUR ENTIRE FACILITY PERIMETER AND MORE

When threats arise, federal and local security operators should be able to rely on their PACS not just to alert them, but act automatically based on custom-implemented security procedures, no matter how complex or straightforward the risk. ReconaSense takes in intelligent security data from all angles, across site locations, and prevents that risk from moving forward.

MAKING SECURITY INTELLIGENT

There are increasingly complicated and intelligent threats in the modern world, as well as outdated systems within the federal sector. Government facilities have an unfulfilled need for intelligent risk-adaptive approaches. ReconaSense accommodates and adjusts in real-time to threats and hazards by unifying security, sensor, IoT devices, and other systems data into a common operating picture. Instead of being reactive, military, federal, and state governments can be proactive with our patented security intelligence platform and risk-adaptive access control solutions.

Contact us today for a comprehensive demo and see first-hand how we can help make your security smarter.

About ReconaSense

ReconaSense® is the first COTS risk-adaptive framework with FICAM certification that can uniquely help identify Insider Threats via real-time data transformation, evaluation and automated policy adjustments. We protect federal, military, state, and other critical infrastructures requiring top-grade security with insider threat detection and our unification platform.

ReconaSense is privately held company headquartered in Austin, Texas.
Visit **www.reconasense.com** to learn more.

Interested in a demonstration?
Email us at **insider@reconasense.com** or call us at **+1 512.220.2010.**

Location

CORPORATE HEADQUARTERS
9130 Jollyville Road
Suite 150
Austin, TX 78759

RECONASENSE

ReconaSense is an American company headquartered in Austin, Texas.